基于标识的证书认证体制CFL
——网络空间认证学及实例

JIYU BIAOSHI DE ZHENGSHU RENZHENG TIZHI CFL
——WANGLUO KONGJIAN RENZHENGXUE JI SHILI

范修斌　刘　昕　王勋龙　杜春玲
戴照鹏　臧鸿雁　王凤瑛　王红兵　著
陈华平　主审

北京邮电大学出版社
www.buptpress.com

基于标识的证书认证体制 CFL
——网络空间认证学及实例

范修斌　刘　昕　王勋龙　杜春玲
戴照鹏　臧鸿雁　王凤瑛　王红兵　著

陈华平　主　审

北京邮电大学出版社
·北京·

图书在版编目(CIP)数据

基于标识的证书认证体制 CFL:网络空间认证学及实例/范修斌等著.
--北京:北京邮电大学出版社,2019.7
ISBN 978-7-5635-5283-2

Ⅰ.①基… Ⅱ.①范… Ⅲ.①计算机网络—认证—研究 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2019)第 037086 号

书　　名	基于标识的证书认证体制 CFL——网络空间认证学及实例
著　　者	范修斌　刘　昕　王勋龙　杜春玲　戴照鹏　臧鸿雁　王凤瑛　王红兵
责任编辑	马飞
出版发行	北京邮电大学出版社
社　　址	北京市海淀区西土城路 10 号(100876)
电话传真	010-82333010　62282185(发行部)　010-82333009　62283578(传真)
网　　址	www.buptpress3.com
电子信箱	ctrd@buptpress.com
经　　销	各地新华书店
印　　刷	北京建宏印刷有限公司
开　　本	787 mm×1 092 mm　1/16
印　　张	9
字　　数	167 千字
版　　次	2019 年 7 月第 1 版　2019 年 7 月第 1 次印刷

ISBN 978-7-5635-5283-2　　定价:54.00 元

如有质量问题请与发行部联系

前　言

本专著的目的是研究网络空间中实体之间相互认证的认证学。本专著共分八章。

为论述网络空间认证学，第一章首先给出关于认证学的基础知识，即可证明安全性理论和零知识证明理论。

为指导网络空间认证学的研究，第二章介绍了什么是信息、香农信息熵，什么是信息安全及信息安全五性；在此基础上，根据当今网络空间的特点，给出了当今网络空间信息安全的八原则，以此作为网络空间认证学研究的前提条件。

第三章给出了网络空间认证学的重要命题，即认证技术是网络空间信息安全第一技术；同时梳理了已有的认证技术。

第四章给出了网络空间认证的目的和本质，继而证明了参数认证或标识认证本质上不具有信息安全功能，例如口令、虹膜、指纹、刷脸、标识等；同时分析了现有函数控制认证技术的不足和缺陷。本章最后给出了信息安全认证体系科学逻辑。

第五章介绍了基于标识的认证体制 CFL 的研发简史、原理以及信息安全属性等。本章最后证明了 CFL 是满足当今网络空间认证体系的科学逻辑的认证体制，也就是说 CFL 在当今网络空间中具有不可替代的作用。

第六章给出了 CFL_BLP 模型的描述和论述，即 CFL 可以充分绑定用户的密钥以及分级分类强制访问控制权限标记，是当前可以充分支持信息系统高等级信息安全建设的认证体制。

第七章以结论的形式论述了 CFL 在当今网络空间中的应用，包括云计算、大数据、智能手机、二维码、物联网、工业 4.0、智慧手机等，也就是说 CFL 作为底层信息安全技术，可以广泛地应用于信息产业中。

第八章鉴于 CFL 技术的核心性、根本性、原点性，给出了基于 CFL 的产业链。

CFL 为标识认证与证书认证混合的认证体制，与已有的认证体制 PKI 与 IBC 相比，CFL 具有一证一钥、多安全根、虎符认证、动态认证、应用去中心、应用去存储、支持现场认证、自主认证、进程认证、节省能耗、边缘计算、支持分级分类强制访问控制、免疫病毒木马、具有主动防御等特点。

针对基于标识的认证体制 CFL，已经发表了十几篇相关学术论文，申请了十八项相关的国家发明专利。来自我国党政军的信息安全专家给出了 CFL“达到

了国际领先水平”的学术鉴定意见。我国相关国家管理机构为 CFL 颁发了红头批文。目前 CFL 已经拥有了相应的应用市场。

感谢本专著合作者的辛勤劳动：

刘昕，中国石油大学(华东)计算机与通信工程学院

王勋龙，青岛海检集团有限公司

杜春玲，山东科技大学信息工程系

戴照鹏，青岛大学数学与统计学院

臧鸿雁，北京科技大学数理学院

王凤瑛，山东科技大学电子信息工程学院

王红兵，国家计算机网络与信息安全管理中心

本专著是在陈华平将军、吕述望教授的具体指导下完成的，在此表示衷心的感谢！

愿 CFL 能够在我国的信息安全实践中发挥应有的积极作用！

范修斌

泰山学院教授

中国科学院软件研究所青岛分部工业信息安全专业委员会主任

北京大学数学科学学院硕士研究生兼职导师

山东科技大学产业教授

青岛大学兼职教授

北京工业大学兼职教授

北京交通大学交通运输学院物流工程专业指导委员会委员

青岛博文广成信息安全技术有限公司首席科学家

山东文斌信息安全技术有限公司首席科学家

中国产学研工匠精神奖获得者

2018 年 10 月 10 日

摘　要

本专著研究了网络空间中实体之间相互认证的认证学。为论述认证学，首先给出了当今网络空间信息安全八原则。以八原则为基础，证明了认证技术是信息安全第一技术。同时证明了参数认证、标识认证（包括口令、指纹、虹膜、刷脸等常规技术）虽具有识别功能，但本质上不具有网络空间中实体之间的认证功能。面对信息安全八原则，原有的认证体制 PKI、IBC 也存在着重大缺陷。

为解决该问题，我们给出了当今网络空间认证体制科学逻辑，并给出了它的实例，即基于标识的认证体制 CFL。在当今网络空间中，CFL 解决了各新兴信息产业共性“卡脖子”问题，具有着不可替代的作用。

Abstract: This monograph studies the mutual authentication between entities in cyberspace. In order to discuss authentication, eight principles of information security in cyberspace are given. Based on the Eight Principles, it is proved that authentication technology is the first technology of information security. At the same time, it is proved that although parameter authentication and identification authentication (including password, fingerprint, iris, face brushing and other conventional technologies) have the recognition function, they do not have the authentication function between entities in cyberspace in essence. Faced with the eight principles of information security, the authentication system PKI and IBC also have major defects.

In order to solve this problem, we present the scientific logic of the authentication system in cyberspace, and give an example of it, that is, the identification —based certificateauthentication system CFL. In today's cyberspace, CFL has solved the common “neck” problem of various information industries, and plays an irreplaceable role.

目　录

第一章　基本知识

为论述网络空间认证学，本章首先给出关于认证学的基础知识，即可证明安全性理论以及零知识证明理论.

1.1　可证明安全性理论

1.1.1　公钥密码算法的可证明安全性理论

公钥密码算法的可证明安全性理论，明确了密码体制的安全定义，建立起一种基本定义、基于归约证明的通用密码学研究方法；通过严格的证明把体制的安全性与已知的计算性难题或密码学关联起来. 可证明安全性理论的研究推进了密码体制的标准化进程，很多标准化组织将密码体制的安全性证明作为密码体制必备的安全属性，要求新提交的密码学标准中的算法能通过安全性证明，目前采用的密码学标准都遵从这种安全规范. 为了给出 CFL 的可证明安全性，作为基础知识，我们首先给出公钥密码算法的可证明安全性理论介绍.

1984 年，戈德瓦瑟(Goldwasser)和米凯利(Micali)在文献[1]中给出了密码学语义安全的概念.

语义安全(semantic security)[1-3]：敌手即使已知某个消息的密文，也得不出该消息的任何部分信息，即使是 1 比特的信息.

这一概念的提出，开创了可证明安全性理论的先河，由密码学信息论安全演进到密码学语义安全.

1.1.1.1　基本概念

公钥加密体制[4]：公钥加密体制 $\Gamma=(K,E,D)$ 一般由以下 3 个多项式时间算法组成：

1)密钥生成算法 K

输入安全参数 k，产生公私钥对 (pk,sk).

2)加密体制 E

输入明文消息 m 和公钥 pk,产生对应的密文 σ.

3)解密算法 D

输入私钥 sk 和密文 σ,输出对应的明文消息 m.

下面介绍公钥加密体制的安全目标层次[4].

对于公钥加密体制的安全目标从低到高(从敌手攻击角度而言指攻破安全体制由难到易)可分为以下几个层次:

1)不可攻破性(unbreakability,UBK)

不可攻破性就是指抗完全攻破. 完全攻破(total break)是从敌手攻击的角度而言的,指敌手能从公钥得到相对应的私钥. 因而完全攻破也称密钥恢复(key covery). 对公钥加密而言公钥总是可以得到的,因而抗完全攻破是一种隐含的基本安全要求.

2)单向性(one-wayness,OW)

从敌手攻击角度而言称为部分攻破(partial break),指敌手可能不知道私钥,但从某些密文能直接得到明文. 更严格地说,抗部分攻破是指在不知道私钥的情况下,从密文不能恢复相应的明文,即敌手 A 成功地对加密体制 E 求逆 D' 的概率是可忽略的,即概率 $Adv_A = P_r(D'(E_{pk}(m) = m))$ 可以忽略. 部分攻破也称为明文恢复(plaintext recovery). 公钥加密的 OW 安全早在 1976 年由迪菲(Diffie)和赫尔曼(Hellman)[5]提出.

3)密文不可区分(indistinguishability,IND)

密文可区分是指攻击者能以超过 1/2 的概率解决以下问题:给攻击者任意 2 个明文和其中任意 1 个明文的密文,攻击者来判断这个密文是 2 个明文中哪一个的密文. 密文不可区分性攻击是判定问题.

4)不可延展性(non-malleability,NM)

不可延展性是指攻击者无法构造与已给密文相关的新密文,即从给定密文不可以构造一个与给定密文对应明文相关的明文的密文. 简言之,从 $Enc(m)$ 不可推出 $Enc(R(m))$,这里 R 是一个非平凡的关系. NM 安全是多列夫(Dolev),德沃克(Dwork)和纳尔(Naor)在文献[8]中提出的. 不可延展性攻击是一个计算问题.

下面介绍敌手的攻击方式[6].

对于公钥加密体制,敌手的攻击方式可分为以下几种:

1)唯密文攻击(cipher only attack,COA)

敌手只能通过考察一些密文来试图推导出解密密钥(即私钥)或这些密文对应的明文.

2)已知明文攻击(known plaintext attack,KPA)

敌手已知一定数量的明文和相对应的密文,试图推导出私钥或者其它密文对

应的明文.

3)非适应性选择明文攻击(chosen plaintext attack,CPA1)

敌手可以选择明文,接着得到这些明文相对应的密文,即假设敌手可访问加密预言(encryption oracle),可以问询这个加密预言机某个明文,从而得到加密预言机的应答,即被问询明文所对应的密文.

4)适应性选择明文攻击(adaptive chosen plaintext attack,CPA2)

敌手可以选择明文,接着得到相应的密文,且明文的选择可依赖于前面得到的密文.

5)非适应性选择密文攻击(chosen ciphertext attack,CCA1)

敌手可以选择密文,接着得到相应的明文,即敌手拥有解密预言机(decryption oracle)的访问权,然后在不访问该解密预言机的情况下,推导出(先前未询问过解密预言机的)密文的明文.

6)适应性选择密文攻击(adaptive chosen ciphertext attack,CCA2)

敌手可以选择密文,接着得到相应的明文,且在见到挑战密文之后还能问询解密预言机.但是,显然不允许向解密预言机问询挑战密文(这里,挑战密文是指需要敌手解密的那个密文).

1.1.1.2　安全模型

加密体制的语义安全概念可由不可区分性(indistinguish ability)游戏(简称IND游戏)来刻画,这种游戏有两个参与者,一个称为挑战者(challenger),另一个是敌手.挑战者建立系统,敌手对系统发起挑战,挑战者接受敌手的挑战.

公钥加密体制在选择明文攻击下的IND游戏(称为IND-CPA游戏)流程如下:

1)初始化

挑战者产生系统 P,敌手获得系统的公钥.

2)挑战

敌手A输出2个长度相同的消息 m_0 和 m_1.挑战者随机选择 $b\in\{0,1\}$,将 m_b 加密,并将密文(称为目标密文)给敌手.

3)猜测

敌手A输出 b',如果 $b'=b$,则敌手攻击成功.

敌手的优势可定义为参数 k 的函数:

$$Adv_{\Gamma,A}^{CPA}(k)=\left|\Pr(b=b')-\frac{1}{2}\right|.$$

其中 k 是安全参数,用来确定加密体制密钥的长度.

定义1[1-6,9-12]　如果对任何多项式时间的敌手A,存在一个可忽略的函数 $negl(k)$,使得 $Adv_{\Gamma,A}^{CPA}(k)\leqslant negl(k)$,那么就称这个加密体制在选择明文攻击下具有不可区

分性，或者称为 IND-CPA 安全.

如果加密体制是确定的，如 RSA 算法、拉宾(Rabin)密码体制等，每个明文对应的密文只有一个，敌手只需重新对 m_0 和 m_1 加密后，与目标密文进行比较，即赢得游戏. 因此语义安全性不适用于确定性的加密体制.

与确定性加密体制相对的是概率加密体制，即在每次加密时，首先选择一个随机数，再生成密文. 因此同一明文在不同的加密中得到的密文不同，如厄格玛尔(ElGamal)加密体制.

ElGamal 加密体制流程描述如下：

1)密钥产生

设 G 是阶为大素数 q 的群，g 为 G 的生成元，随机选择 $x\in \mathbf{Z}_q^*$，计算 $y=g^x \bmod q$，以 x 为私钥，(y,g,q)为公钥.

2)加密

设消息 $m\in G$，随机选一与 $p-1$ 互素的整数 k，计算

$$\begin{cases} c_1=g^k \bmod q \\ c_2=y^k m \bmod q \end{cases}$$

密文为 $c=(c_1,c_2)$.

3)解密

$$m=\frac{c_2}{c_1^x} \bmod q=\frac{y^k m}{g^{kx}} \bmod q=\frac{y^k m}{y^k} \bmod q=m \bmod q.$$

命题 1 ElGamal 加密体制是 IND-CPA 安全的.

证明 在 ElGamal 加密体制的 IND-CPA 游戏中，敌手输出两个长度相同的消息 m_0 和 m_1，挑战者加密 m_b，$b\in\{0,1\}$，得

$$C=(C_1,C_2)=(g^k \bmod p, y^k m_b \bmod p)$$

则

$$\begin{aligned} &\Pr(g^{xk}m_b=g^{xk}m_0) \\ &=\Pr(g^{xk}m_b=g^{xk}m_0,b=0)+\Pr(g^{xk}m_b=g^{xk}m_0,b=1) \\ &=\Pr(b=0)+\Pr(m_1=m_0,b=1). \\ &\Rightarrow \frac{1}{2}\leqslant \Pr(g^{xk}m_b=g^{xk}m_0)\leqslant \frac{1}{2}+negl(k). \end{aligned}$$

$$\begin{aligned} &\Pr(g^{xk}m_b=g^{xk}m_1) \\ &=\Pr(g^{xk}m_b=g^{xk}m_1,b=0)+\Pr(g^{xk}m_b=g^{xk}m_1,b=1) \\ &=\Pr(m_1=m_0,b=0)+\Pr(b=0). \\ &\Rightarrow \frac{1}{2}\leqslant \Pr(g^{xk}m_b=g^{xk}m_1)\leqslant \frac{1}{2}+negl(k). \end{aligned}$$

因此 ElGamal 加密体制是 IND-CPA 安全的.

然而,IND-CPA 安全仅仅保证敌手是完全被动情况时(即仅作监听)的安全,不能保证敌手是主动情况时(例如向网络中注入消息)的安全. 例如敌手收到密文为 $C=(C_1,C_2)$,构造新的密文 $C'=(C_1,C'_2)$,其中 $C'_2=C_2m'$,解密询问后得到明文为 $M=mm'$. 或者构造新的密文 $C''=(C''_1,C_2'')$,其中 $C''_1=C_1g^{k''}$,$C''_2=C_2y^{k''}m''$,此时

$$\begin{cases}C''_1=g^kg^{k''}=g^{k+k''}\\C''_2=y^kmy^{k''}m'=y^{k+k''}mm'\end{cases}$$

解密询问后仍得到 $M=mm'$,再由 $\frac{M}{m}\bmod q$,得到 C 的明文 m. 可见,ElGamal 加密体制不能抵抗此主动攻击.

为了描述敌手的主动攻击,1990 年 Naor 和杨(Yung)[6] 提出了(非适应性)选择密文攻击的概念,其中敌手在获得目标密文以前,可以访问解密预言机. 敌手获得目标密文后希望获得目标密文对应的明文的部分信息.

IND-CCA1 游戏流程如下:

1)初始化

挑战者产生系统 P,敌手 A 获得系统的公开钥.

2)训练

敌手向挑战者(或解密预言机)做解密询问(可多次),即取密文 c 给挑战者,挑战者解密后将明文给敌手.

3)挑战

敌手输出两个长度相同的消息 m_0 和 m_1,再从挑战者接收 m_b 的密文,其中随机值 $b\in\{0,1\}$.

4)猜测

敌手输出 b',如果 $b'=b$,则 A 成功.

敌手的优势可定义为参数 k 的函数,即

$$Adv^{\mathrm{CCA}}_{\Gamma,\mathrm{A}}(k)=\left|\Pr(b'=b)-\frac{1}{2}\right|.$$

定义 2[6]　如果对任何多项式时间的敌手 A,存在一个可忽略的函数 $negl(k)$,使得

$$Adv^{\mathrm{CCA}}_{\Gamma,\mathrm{A}}(k)\leqslant negl(k),$$

那么就称这个加密体制在选择密文攻击下具有不可区分性,或者称为 IND-CCA1 安全.

1991 年,拉科夫(Rackoff)和西蒙(Simon)[12] 提出了适应性选择密文攻击的概

念，其中敌手获得目标密文后，可以向网络中注入消息（可以和目标密文相关），然后通过和网络中的用户交互，获得与目标密文相应的明文的部分信息.

IND 游戏（称为 IND-CCA2 游戏）流程如下：

1）初始化

挑战者产生系统 P，敌手获得系统的公开钥.

2）训练阶段 1

敌手向挑战者（或解密预言机）作解密询问（可多次），即取密文 c 给挑战者，挑战者解密后将明文给敌手.

3）挑战

敌手输出两个长度相同的消息 m_0 和 m_1，再从挑战者接收 m_b 的密文 c_b，其中随机值 $b\in\{0,1\}$.

4）训练阶段 2

敌手继续向挑战者（或解密预言机）作解密询问（可多次），即取密文 $c(c\neq c_b)$ 给挑战者，挑战者解密后将明文给敌手.

5）猜测

敌手输出 b'，如果 $b'=b$，则 A 成功. 敌手的优势可定义为参数 k 的函数：

$$Adv_{\Gamma,A}^{CCA2}(k)=\left|\Pr(b'=b)-\frac{1}{2}\right|.$$

定义 3[12] 如果对任何多项式时间的敌手，存在一个可忽略的函数 $negl(k)$，使得

$$Adv_{\Gamma,A}^{CCA2}(k)\leqslant negl(k),$$

那么就称这个加密体制在适应性选择密文攻击下具有不可区分性，或称为 IND-CCA2 安全.

由文献[13]可知克拉默-舒普（Cramer-Shoup）是 IND-CCA2 安全的加密体制之一，下面对其加以介绍.

Cramer-Shoup 加密体制 $\Gamma=(K,E,D)$ 描述如下：

1）系统建立

设 G 是一个大素数 p 阶的阿贝尔群.

（1）随机选取两个元 $g_1,g_2\in G$；

（2）随机选取 5 个整数 $x_1,x_2,y_1,y_2,z\in[0,p)$；

（3）计算 $c\leftarrow g_1^{x_1}g_2^{x_2}$，$d\leftarrow g_1^{y_1}g_2^{y_2}$，$h\leftarrow g_1^{z}$；

（4）选择哈希（Hash）函数 $H:G^3\mapsto[0,p)$；

（5）公开(g_1,g_2,c,d,h,H)作为公钥，保留行，(x_1,x_2,y_1,y_2,z)作为私钥.

2)加密算法

任意选择一个随机整数 $r\in[0,p)$ 并计算

(1)$u_1\leftarrow g_1^r, u_2\leftarrow g_2^r, e\leftarrow h^r m, \alpha\leftarrow H(u_1,u_2e), v\leftarrow c^r d^m$;

(2)密文为 (u_1,u_2,e,v).

3)解密算法

为解密密文 (u_1,u_2,e,v),执行下列步骤.

(1)$\alpha\leftarrow H(u_1,u_2,e)$,

(2)$\begin{cases} m\leftarrow e/u_1^z, if\ u_1^{x_1+y_1\alpha}u_2^{x_2+y_2\alpha}=v \\ refuse, else \end{cases}$.

记四元组随机变量 $\mathfrak{R}$ 是取值于 G^4 的随机变量,且 $\mathfrak{R}=(g_1,g_2,u_1,u_2)$,其中 $u_1=g_1^{r_1}, u_2=g_2^{r_2}$,$\mathfrak{R}$ 的分布律记为 R.

记四元组随机变量 $\mathfrak{D}$ 是取值于 G^4 的随机变量,且 $\mathfrak{D}=(g_1,g_2,u_1,u_2)$,其中任给 $r\in\mathbf{Z}_q, u_1=g_1^{r_1}, u_2=g_2^{r_2}$ 的分布律记为 D.

一个算法能够解决 DH 判定问题,即能够统计测试区分上述两个分布 R 和 D,也就是说敌手能够以不可忽略的概率判定随机变量来自 R 或 D,即

DH 判定问题是难问题⇔不能在多项式时间内统计测试区分上述两个分布 R 和 D.

DH 判定问题四元组模型到三元组模型的转化:

$$\mathfrak{D}=(g_1,g_2,u_1,u_2)=(g_1,g_2,g_1^r,g_2^r)$$
$$\Rightarrow(g_1=g,g_2=g^x,u_1=g^r,u_2=g^{rx})\Leftrightarrow(g^x,g^y,g^{xy}).$$
$$\mathfrak{R}=(g_1,g_2,u_1,u_2)=(g_1,g_2,g_1^{r_1},g_2^{r_2})$$
$$\Rightarrow(g=g_1,g_2=g^x,u_1=g^{r_1},u_2=g^{r_1r_2})\Leftrightarrow(g^x,g^y,g^z).$$

$g^x=a, g^y=b, g^z=c$,判定 $z=xy$ 是否成立,即要计算

$$g^z=g^{xy}=a^y=c.$$

此处又转化为离散对数问题.

因此,从 DH 判定问题到 DH 问题,从 DH 问题到离散对数问题都是多项式时间的约化关系,但其逆约化关系目前还不清楚.

对于加密算法,$m\in G, E(m)=(g^r,h^rm)$:一方面,如果 DH 判定问题是困难问题,则 h^r 可以由任意群中元代替;另一方面如果 DH 判定问题是可解的,则攻击者对于 (g^r,h^rm_b) 的随机变量 b 具有不可忽略的统计判定优势.

因此可将敌手选择密文攻击的问题转化为统计测试区分分布 R 和 D.

挑战者构造公钥 $pk=(g_1,g_2,c,d,h,H)$ 让 A 使用,并且在他与 A 进行 IND-CCA2 互动时,可以按照 A 的要求构造一条挑战密文 $c=(u_1,u_2,e,v)$,它由选择明

文 m_b 经过加密得到.

在互动过程中,挑战者与 A 将按照如下的方式进行互动:

1)输入$(g_1,g_2,u_1,u_2)\in G^4$,挑战者构造 Cramer-Shoup 体制的一个公钥,将其发送给 A;

2)挑战者与 A 进行互动,挑战者可以对 A 提供的密文进行解密;

3)挑战者从 A 收到 1 对选择明文 m_0,m_1,随机选取 $b\in\{0,1\}$,加密 m_b 构造挑战密文 c,并将 c 发送给 A;

4)挑战者继续为 A 提供解密询问,但是不能对挑战密文 c 进行解密询问;

5)挑战者最后收到 A 对 b 的猜测,然后回答问题$(g_1,g_2,u_1,u_2)=\Re$ 还是$(g_1,g_2,u_1,u_2)=\mathfrak{D}$.

在构造公钥的过程中,挑战者任意选择 $x_1,x_2,y_1,y_2,z_1,z_2\in[0,p)$,并计算

$$c\leftarrow g_1^{x_1}g_2^{x_2},d\leftarrow g_1^{y_1}g_2^{y_2},h\leftarrow g_1^{z_1}g_2^{z_2}.$$

选择 Hash 函数 H,A 要使用的公钥是(g_1,g_2,c,d,h,H).

挑战者使用的私钥为$(x_1,x_2,y_1,y_2,z_1,z_2)$.

对 $h=g_1^{z_1}g_2^{z_2}$,g_1 是 G 的一个生成元,因此对某个 $\omega\in[0,p)$,有 $g_2=g_1^{\omega}$,这样对 $z=z_1+\omega z_2 \bmod p$ 就有

$$h=g_1^{z_1}g_2^{z_2}=g_1^{z_1}g_1^{\omega z_2}=g_1^{z_1+\omega z_2}=g_1^{z},$$

所以 h 服从 Cramer-Shoup 体制.

一旦收到 A 选择的两个明文 m_0,m_1,挑战者就随机选取 $b\in[0,1)$,并按如下方式加密 m_b:

$$u_1=g_1^r,u_2=g_2^r,e=h^rm_b,\alpha=H(u_1,u_2,e),v=c^rd^{r\alpha},$$

即 $e=u_1^{z_1}u_2^{z_2}m_b,v=u_1^{x_1+y_1\alpha}u_2^{x_2+y_2\alpha}$.

得到挑战密文:$c=(u_1,u_2,e,v)$.

解密算法为:$m_b=\dfrac{g_1^{rz_1}g_2^{rz_2}m_b}{g_1^{rz_1}g_2^{rz_2}}=\dfrac{u_1^{z_1}u_2^{z_2}m_b}{u_1^{rz_1+\omega rz_2}}=\dfrac{u_1^{z_1}u_2^{z_2}m_b}{u_1^{z}}=e/u_1^{z}$.

记 $x_1+y_1\alpha=k_1,x_2+y_2\alpha=k_2,k_1+k_2\omega=k_3$,则密文四元组简化如下:

$$\begin{aligned}
c&=(u_1,u_2,e,v)=(g_1^r,g_2^r,g_1^{rz_1}g_2^{rz_2}m_b,c^rd^{r\alpha})\\
&=(g_1^r,g_2^r,g_1^{rz_1}g_2^{rz_2}m_b,(g_1^{x_1}g_2^{x_2})^r(g_1^{y_1}g_2^{y_2})^{r\alpha})\\
&=(g_1^r,g_2^r,g_1^{rz_1}g_1^{\omega rz_2}m_b,(g_1^{rx_1}g_2^{rx_2})(g_1^{ry_1\alpha}g_2^{ry_2\alpha}))\\
&=(g_1^r,g_2^r,g_1^{rz_1}g_1^{\omega rz_2}m_b,(g_1^{rx_1+ry_1\alpha}g_2^{rx_2+ry_2\alpha}))\\
&=(g_1^r,g_1^{\omega rz_1},g_1^{rz}m_b,(g_1^{k_1r}g_2^{k_2r}))\\
&=(g_1^r,g_1^{\omega r},g_1^{zr}m_b,g_1^{k_1r}g_1^{k_2r\omega})\\
&=(g_1^r,g_1^{\omega r},g_1^{zr}m_b,g_1^{k_1r+k_2r\omega})\\
&=(g_1^r=g,g^{\omega},g^{z}m_b,g^{k_3})\Rightarrow(g^{\omega},g^{z}m_b,g^{k_3}).
\end{aligned}$$